Created on 11/16/2004 2:45 PM 20041116A

HAN Guidance – Primary Goals of HAN

Introduction

The **Three Main Objectives** of HAN funding this year are:

1) Continue to make provisions for the ongoing funding and maintenance of Internet and E-mail connectivity.
2) Establish Policies and Security Practices for Computer and Internet/E-mail Use.
3) Plan and further develop your County's or Tribe's local HAN system.

These points are obviously ambitious and we realize that Counties and Tribes have received, and will continue to receive, varying levels of funding from Focus Area E. (i.e., HAN). Fully achieving all three points is the ultimate goal for local public health/medical systems. However, due to varying levels of funding we realize that different local health and emergency response systems will have to develop these capacities at different rates and in different ways. Your agency should start with objective "1" given above (Make provisions for the ongoing funding and maintenance of Internet and E-mail connectivity…) and craft your plan such that it is as fully addressed as possible. Then go on to "2" (Security and Policy Building…) and so on.

Objective 1

For <u>All</u> Health Jurisdictions:

A. Continue making provisions for the ongoing funding and maintenance of Internet and E-mail connectivity for the primary local public health agency, ensuring that this connection is well maintained and that your systems and networks are secured against e-viruses and other threats.

For Health Jurisdictions receiving <u>Total</u> Preparedness funding greater than $50,000.00:

A. Counties and Tribes receiving **<u>Total</u>** BT Preparedness grants greater than $50,000.00 will be required by Focus Area E to submit a HAN plan, line item budget and a timeline (just like last year) for the implementation of their HAN activities. The budget activities should emphasize upgrade of network performance, connectivity and bandwidth. **(See Attachment E for model HAN budget.)**

B. Continue to assist in the extension of Internet and E-mail connectivity to other local public health agencies and allied public agencies that may not have been included so far (e.g., Environmental Health, Sanitarians, EMS, local public health partners, & DES).

Objective 2

For All Health Jurisdictions:

This objective will stress the need for **Security and Policy Building**. This includes the maintenance of infrastructure and the development of policies and procedures implemented at the local level addressing:

A. Computer Workstation Maintenance and Security—Windows Critical Security Updates and Patches, Implementing Hardware or Software Based Firewalls.

- ***a.*** For Large Networks (over 5 computer workstations)—hardware based firewalls are recommended. ***(SummitNet users are behind the State on Montana's firewall so no action is necessary.)***
- ***b.*** For Small Networks (less than 5 computer workstations)—hardware and/or software based firewalls are recommended. ***(SummitNet users are behind the State on Montana's firewall so no action is necessary.)***

B. Anti-Virus Protection—Updating Policies and Procedures

C. Internet/E-mail Use—Acceptable Use Policies/Security Policies

D. Password Policies for: Computer Workstations, Password Change Intervals, Network and Internet Resources

E. Policies regulating Internet Downloads of non-work related software. (i.e. Screensavers, Internet Explorer Toolbars)

F. Technology Upgrade and Hardware Replacement Policy. **(See Attachment D)**

Computer Workstation Maintenance and Security Policy

As an example, all of the computers on the State of Montana's domain are updated with security patches and anti-virus DAT files automatically with the help of some specialized software called Patchlink, which "pushes" critical updates, antivirus updates and security patches to workstations. Many of these issues are taken care of if your agency is on SummitNet. If you have any questions, please contact us. Whether you belong to a large network or a small one these critical updates and anti-virus software updates must be maintained to protect you and your network. A simple policy stating that the Critical updates and Virus DAT files are to be routinely checked for and installed on a certain day at a certain time would be all that's needed to establish a good policy. Larger health jurisdictions may have some or all of these policies in place already. In that case you need only provide us a copy of your current policy/policies.

Acceptable Internet/E-mail Use and Security Policy

The State of Montana's policies enclosed with this guidance regarding ***Acceptable Internet/E-mail Use and Security*** were established to protect the State of Montana, the State of Montana's Network SummitNet and its users. Acceptable Internet Use Policies should include a section on restricting downloads of screen savers, file sharing/swapping software, shareware and freeware such as Internet Explorer tool bars. These policies are established to protect the PC and the network. So-called "Free" software downloaded from the Internet is often packaged with **"Adware"**, **"Spyware"** or infected with computer "**Viruses"**, **"Trojans"** or **"Worms"**. **(See Attachment A page 2 and Attachment C)**

Username and Password Policy

The State of Montana assigns each state employee a unique username (C#) with which the employee uses to access all the state's resources. This unique identifier is also used to track the employee's use of all network resources. County and tribal health agencies should adopt their own username convention and adhere to it. Password policies will have to be tailored to each individual county or tribal health agency. Passwords should be a minimum of 6 characters long and should be changed periodically to insure the security of computer and network resources. **(See Attachment B)**

For <u>All</u> Health Jurisdictions:

A. All Montana county and tribal health agencies will be encouraged to establish written policies regarding acceptable Internet/E-mail Use and Security.

B. All Montana county and tribal health agencies will be encouraged to submit copies of their Security and Internet/E-mail policies to DPHHS.

As the threats of Computer Viruses, Adware, Spam, E-mail Spoofing and Spyware continue so does the job of keeping computer workstations and networks updated and protected, especially when storing sensitive and/or confidential information on local hard drives (i.e. local workstations) or network servers.

Note: Examples of the State of Montana's Internet, E-mail and Username and Password policies will accompany this guidance along with the State of Montana's PC Replacement Policy.

<u>Objective 3</u>

Continue to plan and further develop your County's or Tribe's local HAN system at the local level. This should lead to better integration of communications between members of the local medical system using the Internet and E-mail as their primary platforms for communication. Moreover, when it comes to working with partner and allied agencies on the local level it is not necessary for your agency to purchase everything for the agencies that you will be working with. Your local DES, for example, should be funded through their partners this year. Local hospitals should have funding coming to them through HRSA. DPHHS is administering the HRSA portion of the public health preparedness grant. So your Focus E funds will not need to pay for communications equipment for everyone. However, you and your partner agencies on the local level will get a lot more for your money if you work together and coordinate your spending. Information staff members at DPHHS are available to consult with your local agencies regarding integrated system projects.

For <u>All</u> Health Jurisdictions:

A. Continue to participate in the local expansion of a redundant communications system in coordination with local/regional EMS/DES.

B. Complete the HAN Assessment. The Assessment itself will be provided by DPHHS as part of the 2004-2005 HAN Guidance and will follow closely the quantitative portion of the 2003-2004 Assessment.

Internet, E-mail and other “digitally convergent” communications (i.e., Cell Phones, text messaging, etc.) will continue to represent the core technologies used by the HAN system. Fortunately, the emphasis of both systems (i.e., “radio for DES” and “Internet for HAN”) rather than being limiting, should suggest some options. DES funds should be applied to building/expanding radio communications on the local level using the P25 standard. Whereas HAN funds could be applied to putting an Internet connection into the local DES coordinator’s office, if he/she does not already have one. The DES coordinator could buy a computer using their own funds, to plug into the network connection that HAN had helped fund, thereby closing the loop and giving you both the capacity to communicate through Internet access and E-mail.

Numerous combinations of the above sort are possible, and with regard to helping to create Internet connectivity for local public health agencies and allied organizations, we advocate a cooperative model working outward from a core “public health” center to other related local government agencies and finally to local private/medical health partners. At each step out from the core public health agency, you will need to provide less funding, but will probably have to contribute more to planning. The result should be a net improvement in your jurisdiction’s general capacity to communicate, particularly by E-mail but also by radio, which falls under the category of “redundant communications” within a local HAN.

Contact Information

Jim Aspevig, MS	Gerry Wheat
Public Health Informatics Section - DPHHS	Public Health Informatics Section - DPHHS
WF Cogswell Bldg. Room C-204	WF Cogswell Bldg. Room C-211
1400 Broadway, Helena, MT 59620	1400 Broadway, Helena, MT 59620
Work Cell: (406) 459-9467	Voice: (406) 444-6736
Fax: (406) 444-3044	Fax: (406) 444-3044
E-mail: jaspevig@state.mt.us	E-mail: gwheat@state.mt.us